T08260 "9T659660

Title: Method and Apparatus for Performing Modular Multiplication
Inventor(s): Michael D. Ruehle
Atty. Docket No.: 42390P11975

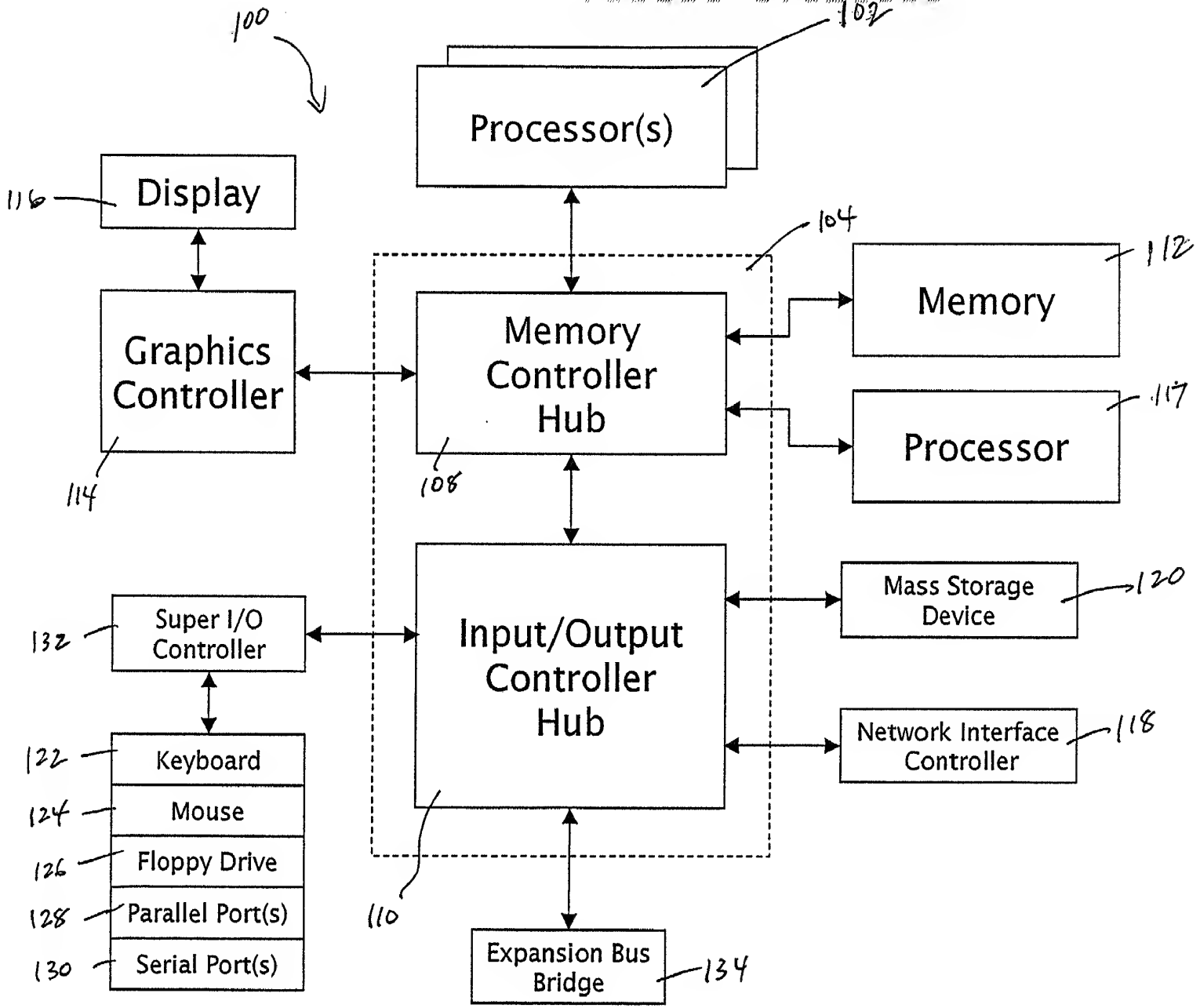

FIGURE 1

10020 S16S960

Title: Method and Apparatus for Performing Modular Multiplication
Inventor(s): Michael D. Ruehle
Atty. Docket No.: 42390P11975

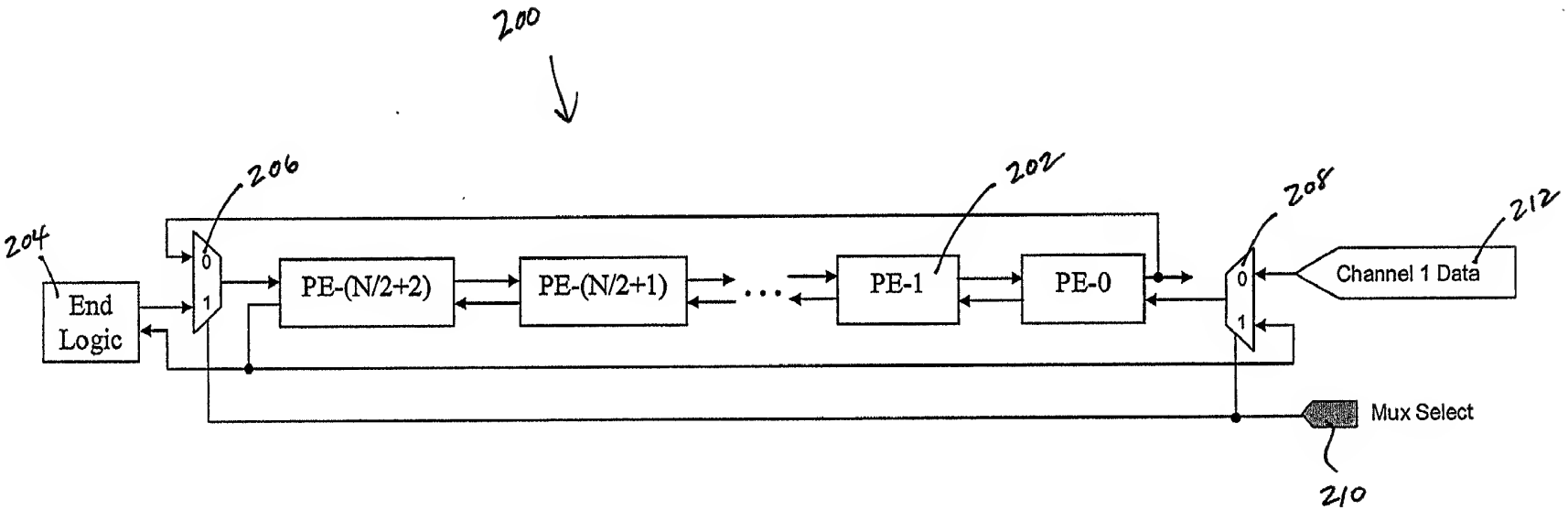

FIGURE 2

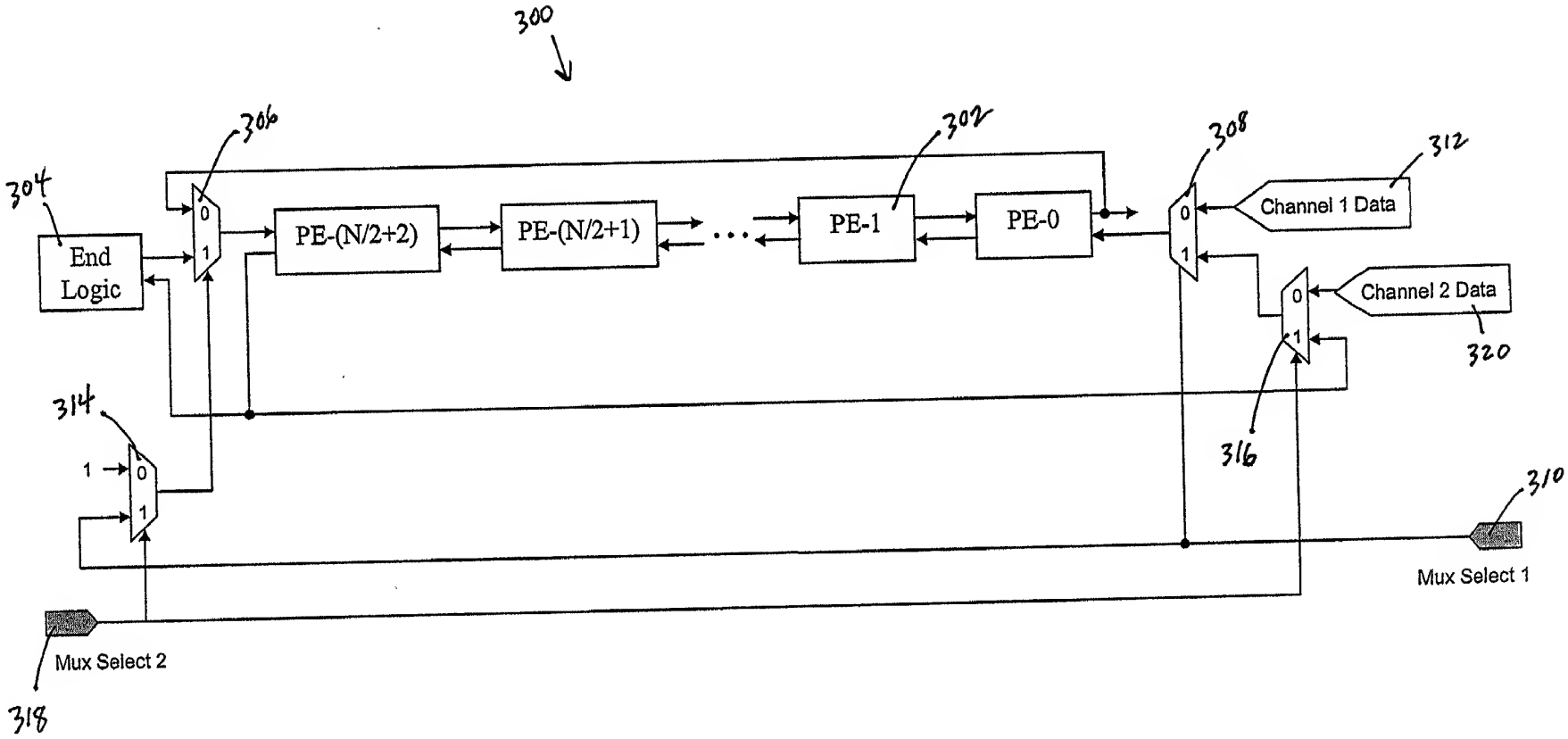
300
304
306
302
308
312
End Logic
PE-(N/2+2)
PE-(N/2+1)
PE-1
PE-0
Channel 1 Data
Channel 2 Data
320
314
316
310
Mux Select 1
Mux Select 2
318

FIGURE 3

Title: Method and Apparatus for Performing Modular Multiplication
Inventor(s): Michael D. Ruehle
Atty. Docket No.: 42390P11975

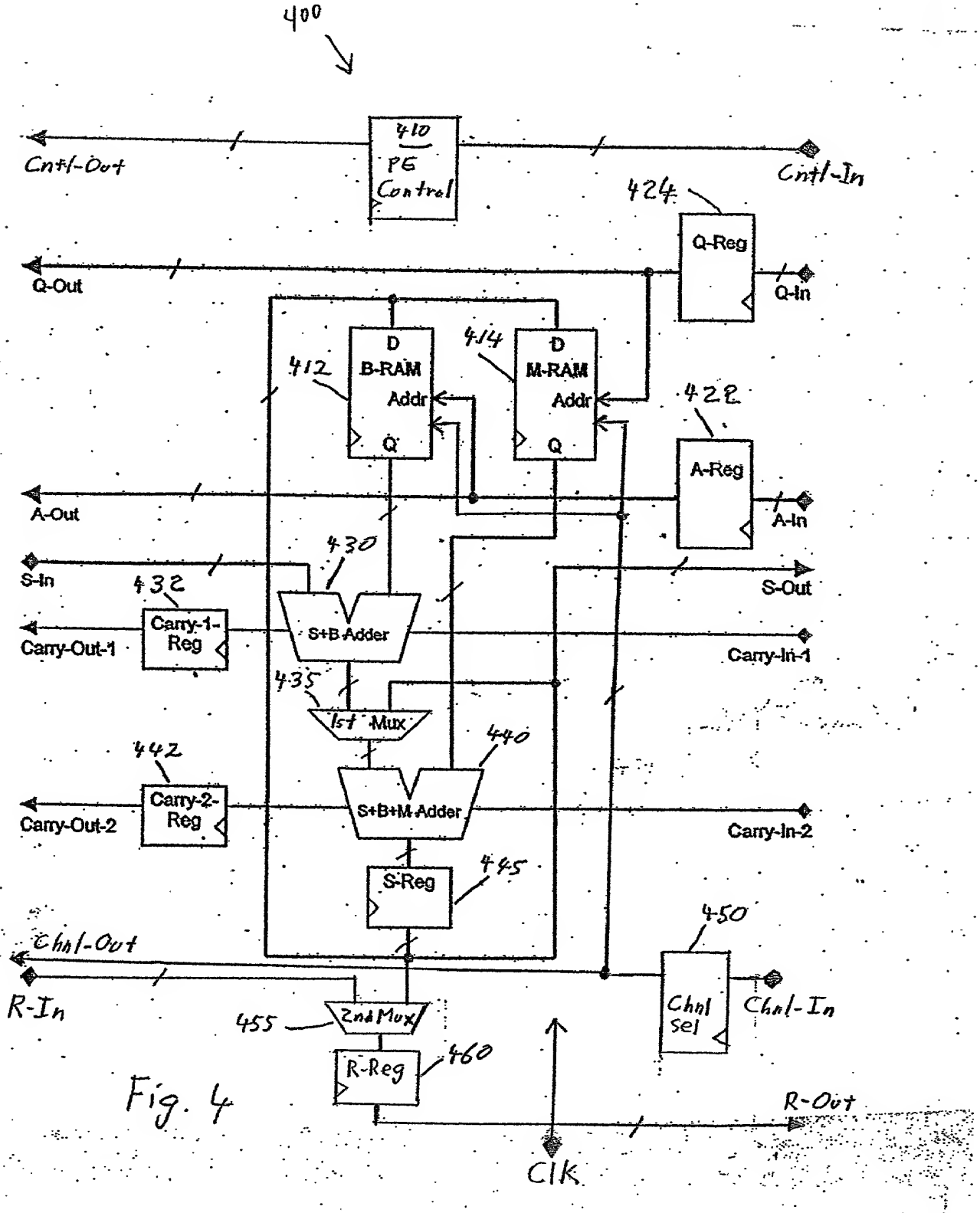

Fig. 4

Cycle	Mux Select	End Logic	PE-6	PE-5	PE-4	PE-3	PE-2	PE-1	PE-0	Input Regs
1	0									
2	1								0	
3	0							1		
4	1						2		0	
5	0					3		1		
6	1				4		2		0	
7	0			5		3		1		
8	1		6		4		2		0	
9	0			5		3		1	7	
10	1		6		4		2	8	0	
11	0			5		3	9	1	7	
12	1		6		4	10	2	8	0	
13	0			5	11	3	9	1	7	
14	1		6	12	4	10	2	8	0	
15	0		13	5	11	3	9	1	7	
16	1		6	12	4	10	2	8	0	
17	0		13	5	11	3	9	1	7	
18	1		6	12	4	10	2	8	0	
19	0		13	5	11	3	9	1	7	
20	1		6	12	4	10	2	8	0	

FIGURE 5

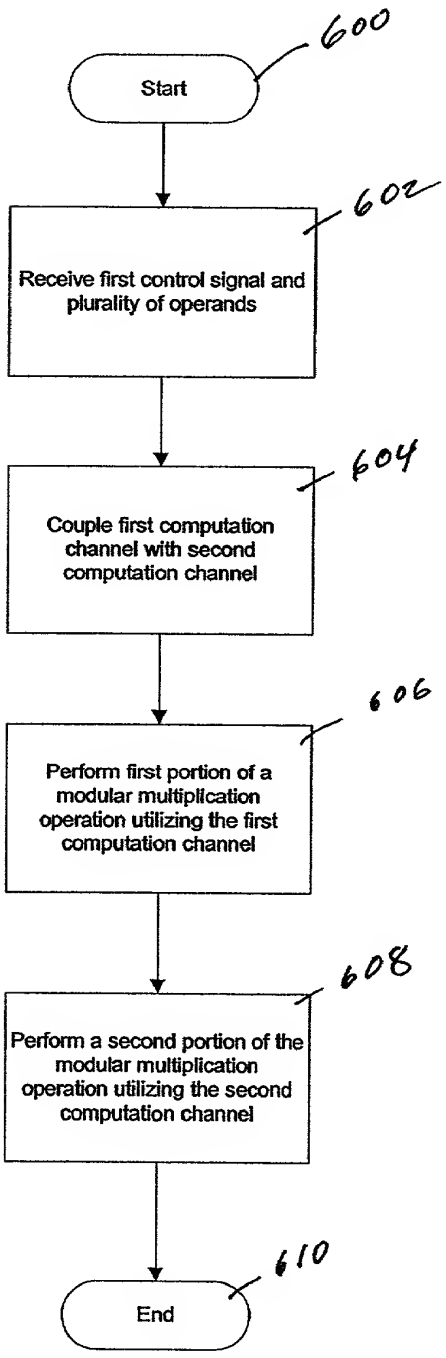
600
Start
602
Receive first control signal and plurality of operands
604
Couple first computation channel with second computation channel
606
Perform first portion of a modular multiplication operation utilizing the first computation channel
608
Perform a second portion of the modular multiplication operation utilizing the second computation channel
610
End

FIGURE 6